Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

# Examining the Role of Organizational Password Security Policies in Individual Password Security Behaviors

Jeannette Kelley
*Temple University*

# Examining the Role of Organizational Password Security Policies in Individual Password Security Behaviors

**Jeannette-Marie Kelley**
Department of Management Information Systems
Fox School of Business and Management
Temple University
jeannette.kelley@temple.edu

**ABSTRACT**

Organizations typically construct computer access password policies that request or require employees to create "strong" passwords. Challenges arise for these employees in attempting to conform to a long list of difficult and potentially conflicting criteria. This dissertation research-in-progress uses concepts from Behavioral Reasoning Theory, General Deterrence Theory, and other theories to examine the conflicting nature of such policies and their impact on password security behaviors. Results are expected to show that traditional countermeasures, while useful in preventing some IS misuse, are not as effective in preventing password misuse, in part because alternative reasons exist that motivate individuals to engage in insecure behaviors. Contributions to academic research and implications for practitioners are discussed.

**Keywords**

passwords, security, IS misuse, password policies, Behavioral Reasoning Theory, General Deterrence Theory

## INTRODUCTION

Organizations typically construct computer access password (PW) policies that request or require employees to create "strong" passwords. Challenges arise for these employees in attempting to conform to a long list of difficult and potentially conflicting criteria. These criteria usually include: passwords should be at least eight or nine digits long; they should be composed of a combination of numbers, letters, and punctuation; they should not include recognizable words, names, or dates; and, they must changed periodically.[1] Policies generally include a list of prohibited behaviors as well as proscribed penalties for violators. However, the effect of these password security policies seems to be that many users, in trying to comply with the difficult and conflicting restrictions, will engage in behaviors that are not secure, such as writing down and sharing passwords.

Research tells us that IS misuse is costly, although the portion attributed to PW misuse is difficult to isolate. According to Campbell et al. (2003) "public disclosure of incidents of unauthorized access resulted in significant drop in stock prices". Insider abuse of network access and unauthorized access by insiders are two of the most severe IS threats (Mehta and George 2001). Recent FBI crime statistics show that approximately 60 percent of industry and government respondents detected costly insider abuse of network security. In recent years, several high-profile breaches of IS security have put a spotlight on the need to protect personal data; legislative mechanisms are being implemented to enforce such protection. Thus it is not surprising that organizations would continuously strive to create security policies that would restrict the ability of individuals (both insiders and outsiders) to access information that needs to be kept secure.

It would appear that the development of password creation guidelines has been largely *ad hoc*: as both computing power and hacker motivation and skills have increased, IT professionals have tried to prevent security breaches by making passwords long, difficult to remember, and short-lived Alternatives to remembering passwords, such as biometrics and RFID tokens, may assist with some of the challenges. However, these are costly, can also be hacked (Furnell 2005), and do not address the behavioral causes of PW misuse. That is, while a technology solution may replace the need to *remember* strong passwords, it will not solve the portion of PW misuse that is volitional: for example, individuals who are motivated to share passwords may be just as likely to share devices.

[1] See, for example, "Sample Password Policy." *Receivables Report for America's Health Care Financial Managers* 20, 7 (2005), 6-7.

IS literature uses several vague and overlapping terms, such as "IS misuse" or "password hygiene", to describe aspects of password behavior. For clarity, the term "password compliance" will be used in this paper. It refers to an individual's *voluntary* adherence to password security guidelines that are communicated by the organization. It specifically does *not* include adherence to these guidelines when such adherence is forced. For example, if a password management program specifically prevents an individual from creating a weak password (by checking new passwords against dictionaries, password histories, and algorithms) then that particular behavior is not part of password compliance.

## THEORETICAL FOUNDATIONS

Several behavioral, cognitive, and economic theories lend important explanations for concepts within IS security and passwords compliance behavior.

*Theory of Reasoned Action (TRA)* (Fishbein and Ajzen 1975) and *Theory of Planned Behavior (TPB)* (Ajzen 1991) establish the connection between an intent to behave in a certain manner and the actual behavior. This is an important linkage in much of the extant IS security literature because many types of IS security breaches are difficult to measure or are kept private by companies who do not wish their security problems to become public knowledge. Thus, while IS researchers generally point to the estimated total dollar value of IS security problems, they are frequently unable to capture data on specific breaches (and their costs). The connection shown in TRA and TPB between "intent" and "actual behavior" allows the assumption that if we can impact individual intent (and its antecedents: attitude, subjective norm, and perceived control), then we can effect a real impact on actual secure behavior.

*General Deterrence Theory*, as used by Straub (1990), shows that severity and certainty of countermeasures (or sanctions) are possible mechanisms to reduce the intent to commit IS misuse, therefore likely reducing actual misuse. Further applying this theory to IS security, D'Arcy (2005) found that countermeasures were effective in preventing certain contemporary types of IS misuse, such as excessive web-surfing during work hours or forwarding of feedback from several respondents. However, password-sharing was dropped from the model in part because feedback from respondents suggested that such sharing was not perceived by them as "IS misuse". Therefore, the concept "IS misuse" needs to be further clarified and the various types of password misuse (e.g., revealing a password, requesting another's password, recording a password in an insecure location, and choosing a weak password) need to be defined and measured. Countermeasures themselves also need to be further clarified. It might be that by solely examining formal, explicit sanctions (e.g., "you will be disciplined or terminated if you engage in IS misuse"), we are ignoring the possible effects of "informal" sanctions (e.g., "if you forget your password, you will be locked out of the system and you may have to interface with the sysadmin"). These informal (or implicit) sanctions may be acting as disincentives for individuals to engage in secure PW behaviors.

A useful method of examining both these formal and informal sanctions arises from *Behavioral Reasoning Theory* (Westaby 2005). This theory incorporates and validates the connections between attitude, intention, and behavior that are shown by TRA and TPB. However, BRT extends the argument by positing antecedents to the "global motives" (attitude, subjective norm, and perceived control); the immediate antecedents of these global motives are "reasons". These reasons are specific to the individual and/or the circumstances; that is, an individual could have an attitude or a perception of a subjective norm that might suggest one behavior but a specific reason may exist why that individual might act contrary to the attitude or norm in a certain circumstance. These specific reasons are shown to impact intention both indirectly (as mediated by global motives) and also directly. An important concept in Behavioral Research Theory is that there can be both reasons "for" and "against" behavior. That is, it subsumes any number of dichotomized dimensions: e.g., pro/con, cost/benefit, facilitating/constraining. Another interesting element of BRT is that it conceives of reasons as "temporally oriented": anticipated (future-looking), concurrent, and *post hoc*. *Post hoc* reasons may be used by individuals to rationalize or justify their actions when those actions are not consistent with their attitudes or other global motives (thus diminishing cognitive dissonance).

*Information Processing Theory (IPT)* (Miller 1956) holds that the maximum number of random characters that individuals can remember is 7 +/- 2. Use of mnemonics and other techniques may assist in the retention of strong passwords in short-term memory. Alternatively, after a period of repetition and coding, a strong password could be passed from short-term memory to long-term memory. Two simultaneous password guidelines do not seem to present serious difficulties. Aytes and Connolly (2004) demonstrate that it is cognitively feasible both to change passwords periodically and also not share passwords; Stanton et al. (2004) show that individuals are readily able to change passwords periodically and also select strong passwords. It appears, however, that attempting to comply with more than two simultaneous restrictions is taxing to individual cognition and therefore causes difficulty in complying with password policies. The cognitive restrictions shown in IPT and these other cognitive studies are likely to be components of the "perceived control" aspect of TRA/TPB and also may exist as *"post hoc"* reasons for non-compliance with password policies, according to BRT.

These theories serve to explain the current relationship between individual reasons, global motives, intention, and behavior. It may be that further extending these arguments to password compliance will afford ample contributions to our knowledge of IS security. However, practitioners may be more interested in not just what these relationships explain, but also what can be done with this knowledge to impact actual IS security. Two additional theories seem to lend assistance:

*Agency Theory* (Alchian and Demsetz 1972) describes the relationship that exists between a principal (i.e., employer) and an agent (i.e., employee) when their goals may conflict. The principal may decide to use a mechanism (e.g., profit-sharing) to encourage the employee to bring his goals in tandem with the employer's goals. A potential application of agency theory to PW misuse is to introduce an incentive that will encourage the employee to engage in secure password behaviors to protect his/her own self-interest, thereby also protecting the employer's security interests.

*Protection Motivation Theory* (Rogers 1983) examines a similar circumstance, in which an individual is interested in preserving his or her own self-interest. However, instead of introducing incentives to encourage certain behavior, the theory says that individuals will seek to protect themselves if they have the knowledge and efficacy to do so and the fear that they could be harmed in some way if they did not take appropriate action. Applying this mechanism to PW compliance, introducing a disincentive might discourage insecure password behaviors and simultaneously protect the organization's security interests. For example, if an employee's password would also allow others to access information that the employee wishes to keep private (e.g., personal information, such as salary), then the employee may be less likely to engage in insecure password behaviors because of the inherent need to protect himself.

The incentives or disincentives suggested by Agency Theory and Protection Motivation Theory are conceptualized as additional "reasons" (for or against compliance). These, along with reasons and concepts that are suggested by the other cited theories will elicit an explanatory model of the various effects of these constructs upon password compliance.

## RESEARCH MODEL AND PROPOSITIONS

General Deterrence Theory suggests that the perceived likelihood and perceived severity of sanctions against IS misuse will have a direct impact on an individual's intention to engage in IS misuse. Applying this reasoning to PW compliance has already been shown to be problematic. It would be useful, however, to perform a more thorough examination to confirm this problem. Such a study would serve as evidence that the previous problem arose from the existence of alternative explanations or is instead due to confusion on the part of participants or incomplete specification of the password-compliance issues. Therefore, the first proposition to be examined is:

> P1: Perceived likelihood and severity of formal sanctions will be positively related to password compliance intention.

If alternative reasons (for or against compliance) exist, this proposition would likely not be supported.

Perceived memory limitations, as a component and antecedent of "perceived control", may impact an individual's intention to comply with password guidelines. That is, if he feels that he cannot remember a password consisting of a large number of unrelated characters, he may be more willing to violate another portion of the password guidelines, such as writing down the password. His perception of his memory constraints is likely a combination of both the number of characters in the password, the length of time that the password is valid, and the number of passwords that need to be remembered. Therefore,

> P2: Perceived memory limitations will be negatively related to several components of password compliance intention, specifically, "choosing a strong password" and "not writing down a password".

Other reasons exist that impact the global motives, the behavioral intent, or both. Some of these reasons exist in standard password guidelines. For example, when guidelines dictate that an employee who forgets her password will be locked out of the system for an extended period of time, she may be more likely to engage in insecure password behaviors because the "cost" of being locked out, or having to wait for or interact with an IT person may be perceived as greater than any likely sanctions.

> P3: Alternative reasons, such as perceived certainty and severity of informal disincentives, will be negatively related to password compliance intention.

Additional reasons could be introduced to create a significant impact upon global motives, behavioral intent, or both. Reasons for or reasons against may introduce enough of a personal stake such that an individual will behave in a way that protects his own self-interest, even if other reasons for or against are not strong enough on their own to have such an effect.

> P4: Personal stake will be positively related to password compliance intention.

The following model highlights the proposed relationships. Additional research suggests the addition of personal characteristics (e.g. age, gender) which are not included here due to space limitations.

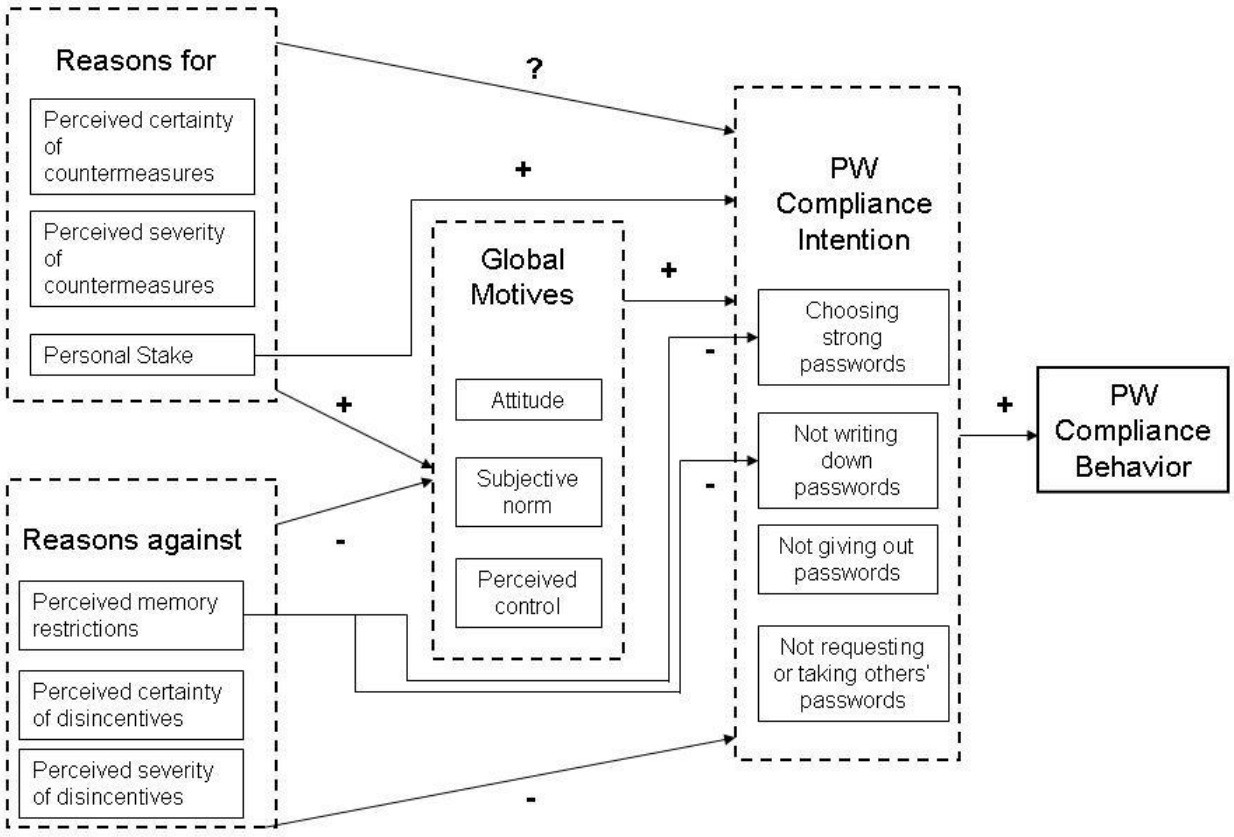


**Figure 1. Preliminary Model**

## METHODOLOGY

Preliminary survey results from over 100 business professionals regarding their password behaviors show correlations between the dependent variable (password misuse) and several independent variables (specifically, length of passwords, frequency of forced password changes, and number of passwords). However, a more rigorous and statistically valid survey is required. Sources of validated survey measures are being explored and potential new measures are being considered. One group of anticipated subjects comes from an industry security group whose members are willing to distribute surveys among co-workers. Surveys will also be administered to employed, part-time MBA students at two major Northeastern universities. Factor analysis and structural equation modeling techniques will be employed for data analysis.

## ANTICIPATED RESULTS AND CONTRIBUTIONS

- Clarification of the password-related components of the "IS misuse" construct.
- Clarification of the effects of explicit and implicit sanctions in deterring IS misuse, especially when they are potentially in conflict.
- Explanation of the limited effects of countermeasures with regard to password security: formal sanctions are ineffective because the strengths of alternative reasons, such as informal disincentives and perceived limitations to memory limitations.

- Demonstration of prescriptive measures for practitioners; introduction of single-password or other mechanisms may encourage employees to engage in secure password behaviors.

**ACKNOWLEDGMENT**

The author would like to thank Dr. Dennis Galletta for his dedicated and outstanding support during the production of this research.

**REFERENCES**

1. Ajzen, I. (1991) The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, 50, 179-211.
2. Alchian, A. A. and Demsetz, H. (1972) Production, information costs, and economic organization, *American Economic Review*, 62, 5, 777-795.
3. Aytes, K. and Connolly, T. (2004) Computer security and risky computing practices: A rational choice perspective, *Journal of Organizational & End User Computing*, 16, 3, 22-40.
4. Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou., L. (2003) The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, *Journal of Computer Security*, 11, 3, 431-448.
5. Fishbein, M. and Ajzen, I. (1975) Belief, attitude, intention, and behavior: An introduction to theory and research, Addison-Wesley, Reading, MA.
6. Furnell, S. (2005) Authenticating ourselves: Will we ever escape the password?, *Network Security*, 2005, 3, 8-13.
7. Mehta, M. and George, B. (2001) Security in today's e-world, in *Proceedings of the Seventh Americas Conference on Information Systems*, August 3-5, Boston, MA.
8. Miller, G. A. (1956) The magical number seven, plus or minus two: Some limits on our capacity for processing information, *Psychological Review*, 63, 81-97.
9. Rogers, R. W. (1983) Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation., in J. Cacioppo and R. Petty (Eds.) *Social psychophysiology*, Guilford Press, New York.
10. Stanton, J. M., K. R. Stam, Mastrangelo, P. R. and Jolton., J. (2004) Behavioral information security: Two end user survey studies of motivation and security practices, in *Proceedings of the Tenth Americas Conference on Information Systems*, August 5-8, New York.
11. Straub, D. W. (1990) Effective is security: An empirical study, *Information Systems Research*, 1, 3, 255-276.
12. Westaby, J. D. (2005) Behavioral reasoning theory: Identifying new linkages underlying intentions and behavior, *Organizational Behavior and Human Decision Processes*, 98, 2, 97-120.